

DES

Crittografia

Luciano Margara

Unibo

2024

Introduzione

Shannon propose di osservare due criteri che sono tuttora alla base dei cifrari a chiave segreta o simmetrici: diffusione e confusione.

Confusione e Diffusione

Confusione e diffusione sono due proprietà della crittografia che un algoritmo di cifratura sicuro deve possedere per essere considerato più o meno robusto, ovvero scarsamente attaccabile da un attacco crittoanalitico. Queste proprietà sono state identificate da Claude Shannon nel suo lavoro La teoria della comunicazione nei sistemi crittografici pubblicato nel 1949.

<https://web.archive.org/web/20070605092733/http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf>

Confusione

Confusione significa che ogni cifra binaria (bit) del testo cifrato dovrebbe dipendere da "tutta" la chiave, oscurando le connessioni tra le due. La proprietà della confusione nasconde la relazione tra il testo cifrato e la chiave. Questa proprietà rende difficile trovare la chiave dal testo cifrato e se viene cambiato un singolo bit in una chiave, il calcolo della maggior parte o di tutti i bit nel testo cifrato sarà influenzato. La confusione è fornita dai "substitution blocks".

Diffusione

Diffusione significa che se cambiamo un singolo bit del testo in chiaro, allora circa la metà dei bit nel testo cifrato dovrebbero cambiare, e allo stesso modo, se cambiamo un bit del testo cifrato, allora circa la metà dei bit del testo in chiaro dovrebbero cambiare. Lo scopo della diffusione è quello di nascondere la relazione statistica tra il testo cifrato e il testo in chiaro. Ad esempio, la diffusione assicura che eventuali pattern nel testo in chiaro, come i bit ridondanti, non siano evidenti nel testo cifrato. La diffusione è fornita dai "permutation blocks".

DES

L'esempio classico di cifrario simmetrico con diffusione e confusione è il Data Encryption Standard, brevemente DES, introdotto dalla IBM nel 1977 e divenuto per ben oltre vent'anni lo standard per le comunicazioni commerciali riservate ma "non classificate".

DES

Nel DES i criteri di Shannon sono soddisfatti attraverso una serie di permutazioni ed espansioni dei bit del messaggio (diffusione), e la combinazione e successiva compressione dei bit del messaggio e della chiave (confusione). Il nucleo di quest'ultima operazione è costituito da un insieme di funzioni raggruppate in un blocco detto S-box da cui dipende crucialmente la sicurezza del cifrario. Si noti che tutte le funzioni impiegate sono immutabili e pubbliche.

DES: la storia

Nel 1972 il National Bureau of Standards (NBS), oggi National Institute for Security and Technology (NIST), ufficio americano per la definizione degli standard, iniziò un programma per proteggere le comunicazioni non classificate, cioè in genere le comunicazioni commerciali o personali fra privati. Il progetto doveva dirigersi verso un sistema di cifratura che presentasse facilità di secretazione della chiave, sicurezza certificata ed economicità nella sostituzione della chiave in presenza di forzature.

DES: la storia

Nel 1973 l'NBS pubblicò un bando che fra i vari punti richiedeva:

- che la sicurezza dell'algoritmo risiedesse nella segretezza della chiave e non nel processo di cifratura e decifrazione
- che l'algoritmo potesse essere realizzato efficientemente in hardware.

DES: la storia

Nessuno avanzò proposte significative. Un bando successivo venne accolto dalla IBM che propose un sistema, il DES, derivato da un software già noto chiamato Lucifer. La National Security Agency (NSA), ente che a quel tempo possedeva tutto lo scibile sulle comunicazioni segrete, certificò il DES, fece commenti sulla sua struttura e propose delle variazioni tra cui la riduzione della lunghezza della chiave da 128 a 56 bit e la modifica delle funzioni contenute nella S-box.

DES: la storia

Tra le motivazioni della NSA vi era la necessità di dissipare ogni possibile dubbio degli utenti sulla presenza di una "porta segreta" nel cifrario, definita dai proponenti per introdursi nelle comunicazioni degli altri, ma diversi utenti replicarono allarmati temendo un'ingerenza proprio della NSA nella costruzione del cifrario

DES: la storia

L'IBM accettò le modifiche solo dopo una severa serie di test i cui criteri sono rimasti segreti. Sembra oggi di poter affermare che il comportamento della NSA era stato corretto: molti dei suoi commenti sono risultati condivisibili da tutti solo quindici anni più tardi. Il DES fu accettato e reso pubblicamente disponibile nel 1977. Con esso finalmente esisteva un cifrario certificato ufficialmente come sicuro, noto a tutti e che tutti potevano studiare con attenzione.

DES: la storia

Il DES doveva essere certificato ogni cinque anni e così avvenne regolarmente fino al 1987, quando ci si chiese se la sua sicurezza fosse ormai messa in pericolo dalle nuove tecniche crittoanalitiche sviluppate nei dieci anni precedenti, nonché dall'aumento di potenza dei calcolatori che rendeva più probabili futuri attacchi esaurienti sull'insieme delle chiavi.

DES: la storia

L'NSA propose nuovi algoritmi realizzati in hardware per sostituire il DES, che non sarebbero dovuti essere pubblici. La proposta non fu ben accettata dalla comunità anche perché poneva seri problemi di riorganizzazione dei sistemi basati sul DES, ormai molto diffusi. Così il cifrario fu certificato di nuovo a più riprese fino al 1999, anno in cui fu dichiarato accettabile solo per scopi limitati ammettendone un uso generale nella versione estesa 3DES. Nel 2005 anche questa versione fu tolta dagli standard, benché sia tuttora utilizzata.

DES: la storia

Nel 1993 il NIST decise di valutare nuove proposte, e nel novembre 2001 scelse il successore denominato AES per Advanced Encryption Standard. Comunque il DES è un pilastro della storia della crittografia e la sua realizzazione è interessante e aiuta anche a comprendere il nuovo cifrario AES.

DES: la struttura

Il messaggio è suddiviso in blocchi, ciascuno dei quali viene cifrato e decifrato indipendentemente dagli altri. Nel DES ogni blocco contiene 64 bit.

Cifratura e decifrazione procedono attraverso r fasi successive (o round) in cui si ripetono le stesse operazioni. Nel DES si ha $r = 16$.

DES: la struttura

La chiave segreta k è composta di b byte. In ciascun byte i primi sette bit sono scelti arbitrariamente e l'ottavo è aggiunto per il controllo di parità. Nel DES si ha $b = 8$, cioè la chiave consta di 64 bit di cui 56 scelti arbitrariamente e 8 di parità.

Dalla chiave k vengono create r sottochiavi $k[0], k[1], \dots, k[r - 1]$ impiegate una per fase.

DES: la struttura

Il messaggio viene diviso in due metà S e D (sinistra e destra). In ciascuna fase si eseguono le due operazioni: $D \rightarrow S$ e $f(k[i - 1], D, S) \rightarrow D$, dove f è una opportuna funzione non lineare e $i = 1, \dots, r$.

Alla fine delle r fasi le due metà vengono nuovamente scambiate e poi concatenate per produrre il crittogramma finale.

DES: la struttura

La decifrazione consiste nel ripetere il processo invertendo l'ordine delle chiavi, caratteristica per nulla ovvia vista la struttura del cifrario.

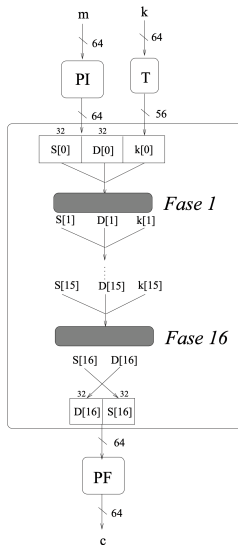
DES: la struttura

Lo schema appena descritto si realizza usando permutazioni di bit, espansioni e compressioni di sequenze binarie e alcune semplici funzioni combinatorie tra messaggio e chiave. L'insieme di queste operazioni garantisce che alla fine del processo ogni bit del crittogramma dipenda da tutti i bit della chiave e da tutti i bit del messaggio in chiaro, rispondendo così ai criteri di confusione e diffusione proposti da Shannon.

DES: la struttura

L'estensione della chiave con i bit di parità garantisce la corretta acquisizione e memorizzazione di tutti i bit della chiave stessa, condizioni cruciali per la decifrazione dell'intero crittogramma. La stessa protezione non è richiesta per il messaggio poiché un errore locale in esso si propaga nel crittogramma, ma è poi riprodotto identico all'originale nel messaggio decifrato con danno in genere irrilevante per la trasmissione.

DES: struttura generale



DES: permutazione PI

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Permutazione PI

il bit 58 dell'input va in posizione 1 dell'output

il bit 50 dell'input va in posizione 2 dell'output

DES: permutazione PF

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Permutazione PF

PF è l'inversa di PI

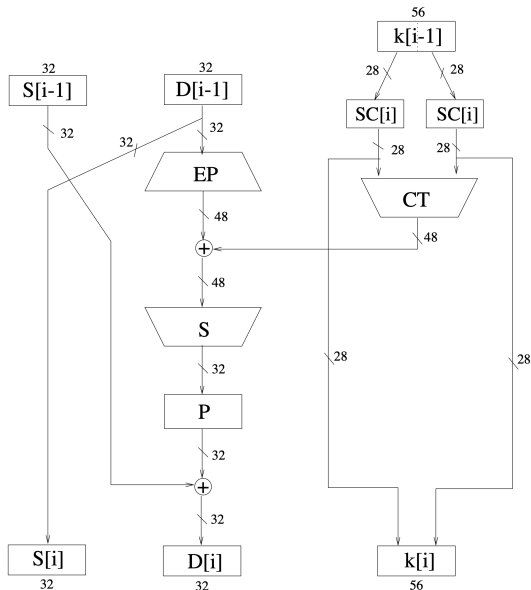
DES: Trasposizione T

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	52	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Trasposizione T

T provvede anche a scartare dalla chiave $k = k_1 k_2 \dots k_{64}$ i bit per il controllo di parità $k_8, k_{16}, \dots, k_{64}$, generando una sequenza di 56 bit che costituisce la prima sottochiave $k[0]$ (si noti che questa tabella ha dimensioni 8×7)

DES: fase i -esima



DES: shift ciclici

La sottochiave $k[i - 1]$ di 56 bit, ricevuta dalla fase precedente, viene suddivisa in due metà di 28 bit ciascuna. Su ognuna di queste la funzione $SC[i]$ esegue uno shift ciclico verso sinistra di un numero di posizioni definito come segue: $SC[i] = 1$ per $i = 1, 2, 9, 16$, $SC[i] = 2$ altrimenti. Le due parti così traslate vengono concatenate in un unico blocco di 56 bit che costituisce la sottochiave $k[i]$ per la fase successiva.

DES: permutazione con selezione CT

14	17	11	24	01	05
03	28	15	06	21	10
23	19	12	04	26	08
16	07	27	20	13	02
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

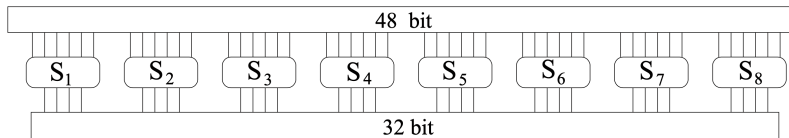
La combinazione delle funzioni $SC[i]$ e CT garantisce che in ogni fase venga estratto dalla sottochiave un diverso sottoinsieme di bit per la cifratura. Si calcola che nella cifratura ogni bit della chiave originale k partecipi in media a 14 fasi.

DES: espansione e permutazione *EP*

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Sedici bit di ingresso vengono duplicati: per esempio il bit 32 è copiato nelle posizioni 1 e 47 dell'uscita.

DES: S-box



$x \backslash y$		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
	1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
	2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
	3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

DES: S-box

Questa funzione, progettata con molta cura dalla IBM e modificata con altrettanta cura dalla NSA, costituisce la parte cruciale e "magica" su cui si basa la sicurezza del cifrario. Essa consta di otto sottofunzioni combinatorie S_1, S_2, \dots, S_8 . L'ingresso di 48 bit viene decomposto in otto blocchi B_1, B_2, \dots, B_8 di 6 bit ciascuno che costituiscono l'ingresso alle sottofunzioni di pari indice.

DES: S-box

Sia $B_j = b_1 b_2 b_3 b_4 b_5 b_6$. Questi bit vengono divisi in due gruppi $b_1 b_6$ e $b_2 b_3 b_4 b_5$ che definiscono due numeri x, y , con $0 \leq x \leq 3$ e $0 \leq y \leq 15$, utilizzati per accedere alla cella di riga x e colonna y in una tabella che definisce la sottofunzione S_j . Il numero ivi contenuto è compreso tra 0 e 15, ed è quindi rappresentato con 4 bit che costituiscono l'uscita di S_j realizzando una compressione da 6 a 4 bit.

DES: S-box

Complessivamente gli otto blocchi generano una sequenza di 32 bit. I blocchi EP e S sono studiati in modo che tutti i bit di $D[i - 1]$ influenzino l'uscita di S , senza di che non sarebbe poi possibile decifrare il messaggio.

DES: permutazione P

<i>16</i>	<i>07</i>	<i>20</i>	<i>21</i>	<i>29</i>	<i>12</i>	<i>28</i>	<i>17</i>
<i>01</i>	<i>15</i>	<i>23</i>	<i>26</i>	<i>05</i>	<i>18</i>	<i>31</i>	<i>10</i>
<i>02</i>	<i>08</i>	<i>24</i>	<i>14</i>	<i>32</i>	<i>27</i>	<i>03</i>	<i>09</i>
<i>19</i>	<i>13</i>	<i>30</i>	<i>06</i>	<i>22</i>	<i>11</i>	<i>04</i>	<i>25</i>

P è una permutazione di 32 bit che genera il blocco finale $D[i]$

DES: linearità e non linearità

Tutte le funzioni applicate dal cifrario, a eccezione della S-box, sono lineari se riferite alla operazione di XOR (\oplus), cioè vale $f(x) \oplus f(y) = f(x \oplus y)$ ove f è una funzione permutazione, espansione o compressione di un vettore binario e x, y sono vettori binari arbitrari. Ciò invece non si verifica se f è una delle otto funzioni della S-box che sono dunque non lineari. Si stima che questo contribuisca in modo determinante alla sicurezza del cifrario.

DES: attacchi

Poiché la chiave è formata da 56 bit si dovrebbero provare in linea di principio tutte le 2^{56} chiavi possibili. Alcune osservazioni sulla struttura del cifrario permettono però di ridurre leggermente lo spazio da esplorare.

$$2^{56} = 36.028.797.018.963.968$$

Per dimezzare l'insieme delle chiavi si noti che

$C(m, k) = c$ implica $C(\overline{m}, \overline{k}) = \overline{c}$, ove la barra indica la complementazione bit a bit di una sequenza binaria

DES: confusione e diffusione

```
TestPlaintext[] :=  
Module[{again, c1, c2, plaintext2, pos, plaintext1, key},  
  plaintext1 = IntegerDigits[RandomInteger[{0, 2^64 - 1}], 2, 64];  
  key = IntegerDigits[RandomInteger[{0, 2^64 - 1}], 2, 64];  
  pos = RandomInteger[{1, 64}];  
  plaintext2 = plaintext1;  
  If[plaintext2[[pos]] == 0, plaintext2[[pos]] = 1, plaintext2[[pos]] = 0];  
  c1 = DES[plaintext1, key];  
  c2 = DES[plaintext2, key];  
  Return[HammingDistance[c1, c2]]  
]
```

DES: confusione e diffusione

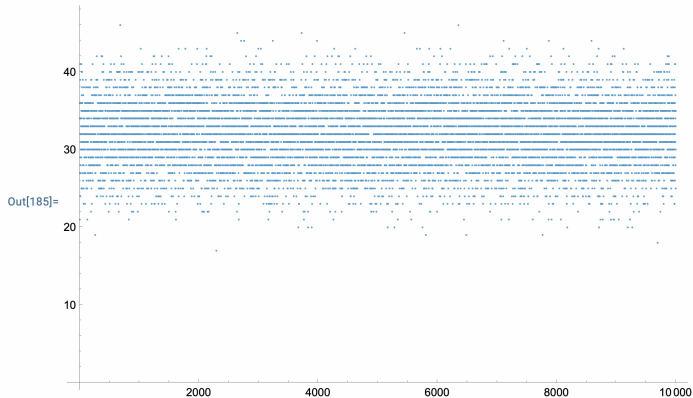
```
TestKey[] :=  
Module[{again, c1, c2, pos, plaintext, key1, key2},  
  plaintext = IntegerDigits[RandomInteger[{0, 2^64 - 1}], 2, 64];  
  key1 = IntegerDigits[RandomInteger[{0, 2^64 - 1}], 2, 64];  
  Label[again];  
  pos = RandomInteger[{1, 64}];  
  If[pos == 8 || pos == 16 || pos == 24 || pos == 32 || pos == 40 || pos == 48 || pos == 56 ||  
    Goto[again]  
];  
  key2 = key1;  
  If[key2[[pos]] == 0, key2[[pos]] = 1, key2[[pos]] = 0];  
  c1 = DES[plaintext, key1];  
  c2 = DES[plaintext, key2];  
  Return[HammingDistance[c1, c2]]  
]
```

DES: confusione e diffusione

```
pt = Table[TestPlaintext[], 10 000];  
k = Table[TestKey[], 10 000];
```

DES: confusione e diffusione

```
In[185]:= ListPlot[pt]
```

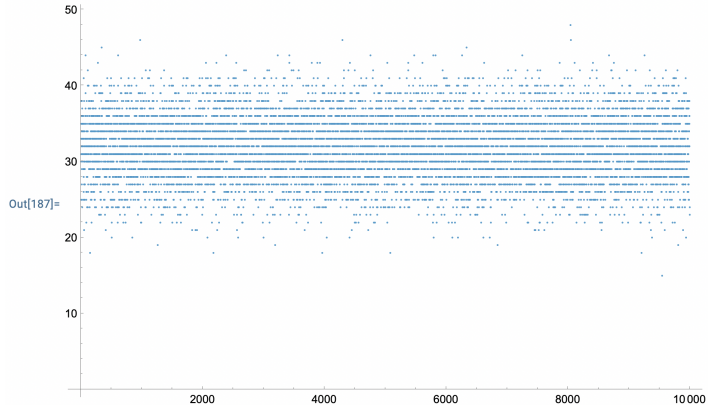





```
In[186]:= Mean[pt] // N
```

```
Out[186]= 32.0273
```


DES: confusione e diffusione

In[187]:= ListPlot[k]



theme... frame... labels... axes ▾ more...   

In[188]:= Mean[k] // N

Out[188]= 31.9801